

## Re: Checkpoint experiences

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2003-10/0710.html>

---

**From:** Beoweolf (*Beoweolf-spam\_at\_pacbell.net*)

**Date:** 10/10/03

Date: Fri, 10 Oct 2003 05:03:28 GMT

Nothing you said in the below message is a surprise. You don't buy a tractor to run the Indy 500, a bus to pop by the local 7-11 for a pack of smokes or a Yugo to impress your in-laws. That would be inappropriate use for the design...same with firewalls, buy what you need, not what you want. You will be happier and the lame ass CS techs won't have to guess nearly so much. in their defense, you have to admit..Checkpoint full install covers a lot of ground 6 major OS, 3 platforms and a host of possible configurations.

Many people hear that Checkpoint is #1 in enterprise level firewalls and decide they want the firewall used by the big boys...often repeated, but seldom heard...Checkpoint is not for everyone! It is not a consumer oriented firewall. The Nokia appliance IPSO, is useful if you don't want to take the time to build or buy and configure a server yourself. It comes with a pre hardened OS (a variant of Unix), a management interface voyager, an enforcement module and pre installed Checkpoint. You still need to configure it and know something about how your network is setup (IP addresses, routers, swatches etc. This is not something that should be a burden, as an administrator you should have than information documented in text and some kind of graphic template available if not tattooed inside your brain.

I am not one of those old timers that complain because things are too easy, but lets be serious here folks...if you are going to administer a network and secure it from internet assaults, you need to be at least 1/2 as smart as the hackers. It isn't always the other guys fault when you buy the wrong thing or get in over your head. Do your own research before purchasing anything, if it doesn't fit your situation, then don't buy it. If you screw it up, then read a manual, buy a book, take a class...whatever it takes to grasp the technology. Never throw up you hands and give up without a fight. Believe it or not, you learn more from near failure than from easy installs.

"john dobbs" <jdobbs2001@yahoo.com> wrote in message  
news:9e63d1b0.0310091206.26e997ba@posting.google.com...

> *From: Molalla Attenborough (none@noplaceever.net)*

> *Subject: Nokia/Checkpoint Nightmare*

> *View: Complete Thread (12 articles)*

> *Original Format*

> *Newsgroups: comp.security.firewalls*

> *Date: 2003-04-08 10:05:36 PST*

>  
>  
> *I hereby declare that I will never, ever recommend a Nokia/Checkpoint to  
> anyone other than my worst IT enemy. If you are a small company, do please  
> do your homework before going this route. The Nokia/Checkpoint route is  
> fraught with danger. It is no wonder that the Nokia interface is called  
> Voyager, since you will embark upon a journey trying to configure it. I  
want  
> a firewall with interface software called Sofa. I don't want a journey. I  
> just want to sit in my command seat with the remote and make things work  
> with the minimum amount of effort while I eat a Krispy Kreme.*  
>  
>  
>  
> *Now, on to the story.*  
>  
>  
>  
> *I currently work for a medium size business. We have pretty basic  
> requirements. We have under 100 users, a web site, an FTP site, a SMTP  
> gateway, a couple of VPN users, etc. Not unlike a zillion other companies  
> out there.*  
>  
>  
>  
> *We currently have a Watchguard Firebox as our firewall. I didn't purchase  
> it. I come from a PIX background at a much larger company. But, the  
Firebox  
> was here when I got here. It's actually a great little unit. It has very  
> helpful tools and software, it's pretty easy to set up and maintain. The  
> problem is this: It has died on us twice in a year and has had to be  
> replaced. It will just fail to come back up after a reboot. It's like it  
> gets sleepy and needs a rest after working hard for a bit. If you reboot  
it  
> 15 or 20 times while holding factory reset, it will usually come back up.  
> Not exactly the warm, fuzzy feeling of set and forget I am looking for in  
my  
> firewall.*  
>  
>  
>  
> *Anyway, because of the above, we were looking for a replacement. We don't  
> have a huge budget. So, we started looking. I had always heard good things  
> about Nokia/Checkpoint solutions. Well, let me re-phrase. I had heard  
these  
> things from IT peers working at BIG companies. Companies that will spend  
> billions on training, and classes, consultants, support contracts, etc.*  
>  
>  
>  
> *So, I saw that the Nokia IP120 "Appliance". Now, when I think of*

appliance,

> *I think of my toaster. Or, my washer and dryer. My microwave. Nokia*

> *optimistically refers to the IP120 as an "appliance". Well, if Nokia built*

*a*

> *toaster it would work like this:*

>

> *1) It would be a distributed solution where you had to license the*

*toaster,*

> *the bread, the electricity and the number of people in your house that*

*could*

> *enjoy toast.*

>

> *2) If the number of people in your house exceeded the license count of the*

> *"appliance" regardless of whether the people actually ate toast or not,*

*the*

> *"appliance" would cease to function.*

>

> *3) The toaster would have a yearly support contract for the toaster. They*

> *would tell you that the bread support was included but you would later*

*find*

> *they know very little about bread and nothing about the baking process in*

> *general.*

>

>

>

> *But I digress. Back to the story...*

>

>

>

> *The Nokia/Checkpoint "solution" is comprised of a piece of hardware made*

*by*

> *Nokia and software made by Checkpoint. Some of the software comes bundled*

*on*

> *the "appliance" in the form of modules that need keys to unlock the*

> *functionality. You also get software of various sorts and types from*

> *Checkpoint. One of the first decisions that you have to make is what IP*

> *address you want to use during the licensing process. Why? Because, it is*

> *used as part of the key generation process.*

>

>

>

> *What does this mean? It means that MUST use an ip address that will be*

*used*

> *one of the interfaces of the install. But wait. What they don't tell you*

*up*

> *front is that there are STAND ALONE and DISTRIBUTED installations.*

> *Basically, a stand alone installation has the enforcement module and the*

> *management module both activated on the Nokia device but when you talk to*

> *the techs they tell you that you are better off with the distributed*

> *installation which means that you activate the enforcement module only on*

> *the Nokia "Appliance" and the management workstation on a some other*

## comp.security.firewalls: Re: Checkpoint experiences

> *computer which is when you find out for the first time that the IPs you used*

> *for your licensing are WRONG and you need to go to their website to*

> *re-license and then reactivate the "appliance". (Whew)*

>

>

--

> -----

>

> WARNING: Devices that require classes before setup are only suitable if you

> are working for a big company and you want to buy a device that ensures your

> job for at least a year while you figure out how this stuff works.

>

> -----

--

> -----

>

>

>

>

> All right, now to the meat of our problem. Also, please remember, I am pretty much of a guy that can get stuff installed in a short period of time

> if I am working with a well documented, well supported product. Here is what

> I wanted to do...

>

>

>

> I wanted:

>

> 1) Two public IP addresses exposed on the outside interface of the firewall

>

> 2) A DMZ with a SMTP server, an FTP server, and a Web server

>

> 3) An internal network. We occasionally will punch tight holes through the firewall to allow access to individual hosts/services inside.

>

>

>

> Not complicated right? I have done this kind of setup on a PIX and on the Watchguard. When I began to configure the Nokia/Checkpoint appliance, I immediately ran into problems. This required me to call the support center.

>

>

>

> Ahhh. The Nokia support line. Such fond memories. Over the last 4 days I have had no less than 6 incidents opened and closed around my simple problem. I have received different answers almost ever time I call. I have been insulted and sneered at. And, I have received a deathblow (More in a minute)

>

>

>

> What could cause such confusion? Here is the question I posed to them.

## comp.security.firewalls: Re: Checkpoint experiences

>  
>  
>  
> Me: Hi. I need to set up the Nokia so that it has 2 public IP's on the  
> external interface and I want to map specific ports on those IPs to  
> different hosts in my DMZ and possibly internal network. How do I do this?  
>  
>  
>  
> This seems like an innocent question. It seems easy to since on the  
Firebox,  
> for instance, I just go to the tab called NETWORK SETUP and then ALIAS and  
> add an IP to the interface. Then I do a little NAT and bad-a-bing if  
someone  
> knocks on port 25 of one of my outside interface IP's I send them to port  
25  
> of our mail gateway(10.0.0.25) in the DMZ. If someone knocks on port 21 of  
> that same outside interface, I send them to port 21 of out FTP server  
> (10.0.0.21) in the DMZ. All is happy, all is good, all is easy.  
>  
>  
>  
> Here are the answers I got from Nokia.  
>  
> 1) You can't do that  
>  
> 2) You can't do it but you need to do static NAT  
>  
> 3) You can't do it with static NAT  
>  
> 4) You need to set up static ARP entries  
>  
> 5) You don't need static ARP entries  
>  
> 6) You need to setup NAT using the NAT tab of the network object  
>  
> 7) You shouldn't use the NAT tabs, you should setup manual NAT  
>  
> 8) Why do you want to do that?  
>  
> 9) Just look at these (useful but inapplicable) knowledge base articles  
>  
>  
>  
> I was also told by one "helpful" Nokia rep that they didn't do  
> "walkthroughs" of this type and he suggested I enroll in some NG classes  
for  
> training.  
>  
>  
>  
> REALITY CHECK: I want to get this thing up and running while sucking a  
> Starbucks Carmel Machiato and working on my latest VB.NET/SQL project for  
> the company. I am now insulted, confused, pissed off, and kind of  
> disappointed. Now, the deathblow...  
>  
>  
>  
> I finally talked to a guy at Nokia who knew what he was talking about. The  
> range of knowledge of the techs was astounding. It ranged from ignorant to  
> brilliant. Unfortunately, that's the sort order I got. I talked to the  
> brilliant one last. His name was something like Mansoon.

## comp.security.firewalls: Re: Checkpoint experiences

>  
>  
>  
> He set me straight on a couple of key points.  
>  
> 1) We have a 50 user license. No one told me that the Nokia/Checkpoint  
> solution will scan my network for IP's of ANYTHING, hosts, workstations,  
> printers, wireless hubs in our warehouse, etc and all of these will go  
> against the license count. Even if I have under 50 USERS the printers will  
> count and if the count is exceeded the device will begin scrolling a  
message  
> in itself that acts like a self inflicted denial of service attack and it  
> basically shuts down  
>  
> 2) If I want to add another IP address to the outside interface, I will  
need  
> more licenses from Chekpoint!!!!!!!!!!!!!!  
>  
>  
>  
> That was it. The deathblow. I cannot confirm if he was right or wrong. I  
> don't want to. We are packing up the box as I write this. It is going  
back.  
> I never, ever, ever, ever, ever want to see another box with Nokia or  
> Checkpoint on it again. Ever. Ever.  
>  
>  
>  
>  
> PS: I made one call to a company called Netscreen. My call was answered. I  
> asked for pre-sales technical support. I was connected immediately to a  
> gentleman who listened to my story. I asked him the same above question  
> about my architecture. He said none of this was any problem. He pointed me  
> at a Netscreen 25 which has 4 interfaces, unlimited users and I can pick  
up  
> a 100 user VPN pack for about \$195. He showed me a web demo of the  
software  
> which looks good (I must admit, not as cool as the Watchguard) but  
adequate.  
> Maybe I'll get that Krispy Kreme soon...  
>  
>  
>  
>  
>  
> PPS:  
>  
> A note on Watchguard. The software is cool, the hardware is flaky and the  
> support lines are AWFUL.  
>  
>  
>  
>  
>  
> PPPS: I will follow up in a few days and post how it goes with the  
Netscreen  
> product...  
---

Outgoing mail is certified Virus Free.  
Checked by AVG anti-virus system (<http://www.grisoft.com>).  
Version: 6.0.524 / Virus Database: 321 - Release Date: 10/6/2003